SPECIALIZATION RESULTS IN GALOIS THEORY

PIERRE DÈBES AND FRANÇOIS LEGRAND

Abstract. The paper has three main applications. The first one is this Hilbert-Grunwald statement. If $f : X \to \mathbb{P}^1$ is a degree n $\mathbb{Q}$-cover with monodromy group S_n over $\overline{\mathbb{Q}}$, and finitely many suitably big primes p are given with partitions $\{d_{p,1},\ldots,d_{p,s_p}\}$ of n, there exist infinitely many specializations of f at points $t_0 \in \mathbb{Q}$ that are degree n field extensions with residue degrees $d_{p,1},\ldots,d_{p,s_p}$ at each prescribed prime p. The second one provides a description of the separable closure of a PAC field k of characteristic $p \neq 2$: it is generated by all elements y such that $y^m - y \in k$ for some $m \geq 2$. The third one involves Hurwitz moduli spaces and concerns fields of definition of covers. A common tool is a criterion for an étale algebra $\prod_l E_l/k$ over a field k to be the specialization of a k-cover $f : X \to B$ at some point $t_0 \in B(k)$. The question is reduced to finding k-rational points on a certain k-variety, and then studied over the various fields k of our applications.

1. Introduction

The paper has three main applications which all are specialization results in Galois theory.

A first one is the following version of Hilbert's irreducibility theorem where a Grunwald like conclusion is conjoined with the usual irreducibility conclusion.

Theorem 1 (corollary 4.1) *Let $f : X \to \mathbb{P}^1$ be a degree n $\mathbb{Q}$-cover with geometric monodromy group*[1] *S_n and S be a finite set of primes p, suitably large (depending on f), each given with some positive integers $d_{p,1},\ldots,d_{p,s_p}$ of sum n. Then f has infinitely many specializations that are degree n field extensions of $\mathbb{Q}$ with residue degrees $d_{p,1},\ldots,d_{p,s_p}$ at each $p \in S$.*

Date: July 1, 2011.

2000 *Mathematics Subject Classification.* Primary 11R58, 12E30, 12E25, 14G05, 14H30; Secondary 12Fxx, 14Gxx, 14H10.

Key words and phrases. Specialization, algebraic covers, twisting lemma, Hilbert's irreducibility theorem, Grunwald's problem, PAC fields, local fields, global fields, Hurwitz spaces.

[1] that is: the Galois group of the Galois closure of f over $\overline{\mathbb{Q}}$.

A second one is concerned with the arithmetic of PAC fields. Recall that a field k is said to be PAC if every non-empty geometrically irreducible k-variety has a Zariski-dense set of k-rational points. A typical example is the field $\mathbb{Q}^{\mathrm{tr}}(\sqrt{-1})$ (which is also hilbertian and whose absolute Galois group is a free profinite group of countable rank); here $\mathbb{Q}^{\mathrm{tr}}$ is the field of totally real numbers (algebraic numbers such that all conjugates are real). See [FJ04] for more on PAC fields.

Theorem 2 (corollary 4.3) *If k is a PAC field of characteristic p, every extension E/k of degree n with $p \not| n(n-1)$ can be realized by a trinomial $Y^n - Y + b \in k[Y]$. Furthermore, if $p \neq 2$, the separable closure k^{sep} is generated by all elements $y \in k^{\mathrm{sep}}$ such that $y^n - y \in k$ for some $n \geq 2$.*

We have similar applications about realizations by Morse polynomials (corollary 4.4), and over finite fields (§4.2.3).

A third application concerns Hurwitz moduli spaces of covers of $\mathbb{P}^1$ with fixed branch point number r and fixed monodromy group. Let H be a geometrically irreducible component of some Hurwitz space defined over some field k and N be the degree of the field of definition of the generic cover in H over that of its branch point divisor; more formally N is the degree of the natural cover $\mathsf{H} \to \mathsf{U}_r$ with U_r the configuration space for finite subsets of $\mathbb{P}^1$ of cardinality r (see §4.3). We also make this assumption which can be checked in practice: the Hurwitz braid action restricted to H generates all of S_N (more formally S_N is the geometric monodromy group of the cover $\mathsf{H} \to \mathsf{U}_r$).

Theorem 3 (corollary 4.6) *Consider the subset $\mathcal{U} \subset \mathsf{U}_r(k)$ of all $\mathbf{t}_0$ such that the $\overline{k}$-covers $f : X \to \mathbb{P}^1$ in H with branch divisor $\mathbf{t}_0$ satisfy the following condition* (in each case)*:*

(a) (case k PAC of characteristic 0)*: their smallest fields of definition are given finite extensions E_l/k $(l = 1, \ldots, s)$ with $\sum_{l=1}^{s} [E_l : k] = N$,*

(b) (case k a number field)*:*

- their fields of moduli are degree N extensions of k, and

- for each v in a given finite set of finite places of k with suitably big residue field and residue characteristic (depending on H), and each associated partition $\{d_{v,1} \ldots, d_{v,s_v}\}$ of N, the smallest definition fields of the covers $f \otimes_{\overline{k}} \overline{k_v}$ are the unramifed extensions of k_v of degree $d_{v,1}, \ldots, d_{v,s_v}$.

Then (in each case) *$\mathcal{U}$ is a Zariski-dense subset of $\mathsf{U}_r(k)$.*

We refer to §4 for more detailed statements and further applications.

A common tool for these applications is a general specialization result. If $f : X \to B$ is an algebraic cover defined over a field k and t_0 a

k-rational point on B, not in the finite list of branch points of f, the specialization of f at t_0 is defined as a finite k-étale algebra of degree $n = \deg(f)$. For example, if $B = \mathbb{P}^1$ and f is given by some polynomial $P(T,Y) \in k[T,Y]$, it is the product of separable extensions of k that correspond to the irreducible factors of $P(t_0, Y)$ (for all but finitely many $t_0 \in k$). The central question is whether a given k-étale algebra of degree n is the specialization at some unramified point $t_0 \in B(k)$ of some given degree n k-cover $f : X \to B$. The classical Hilbert specialization property corresponds to the special case étale algebras are taken to be single field extensions of degree n and the answer is positive for at least one of them.

The question was investigated in [Dèb99c] and [DG11] for Galois covers and some answers given that relate to the Regular Inverse Galois Problem (RIGP) and the Grunwald problem. We consider here the situation of not necessarily Galois covers. Our main tool is a *twisting lemma* which extends the twisting lemma from the previous papers and gives a general answer to our question, under some hypothesis. The answer is that there exists a certain "twisted" cover $\widetilde{g} : \widetilde{Z} \to B$ such that the étale algebra *is* a specialization of the cover at some point $t_0 \in B(k)$ if there exist unramified k-rational points on $\widetilde{Z}$ (lemma 2.1). The hypothesis is that the geometric monodromy group of the cover f is the symetric group S_n where $n = \deg(f)$; it is satisfied in many practical situations.

In §3 we investigate the remaining problem of finding rational points on $\widetilde{Z}$ over various fields: PAC fields, finite fields, complete fields, number fields. Corollaries 3.1 - 3.4 are answers to the original question in these situations. Applications are finally proved in §4.

2. The twisting lemma

2.1. **Basic notation.** Given a field k, fix an algebraic closure $\overline{k}$ and denote the separable closure of k in $\overline{k}$ by $k^{\rm sep}$ and its absolute Galois group by G_k. If k' is an overfield of k, we use the notation $\otimes_k k'$ for the scalar extension from k to k': for example, if X is a k-curve, $X \otimes_k k'$ is the k'-curve obtained by scalar extension. For more on this subsection, we refer to [DD97, §2] or [Dèb09, chapitre 3].

2.1.1. *Etale algebras and their Galois representations.* Given a field k, a *k-étale algebra* is a product $\prod_{l=1}^{s} E_l/k$ of k-isomorphism classes of finite sub-field extensions $E_1/k, \ldots, E_s/k$ of $k^{\rm sep}/k$. Set $m_l = [E_l : k]$, $l = 1, \ldots, s$ and $m = \sum_{l=1}^{s} m_l$. If N/k is a Galois extension containing the Galois closures of $E_1/k, \ldots, E_s/k$, the Galois group $\mathrm{Gal}(N/k)$ acts by left multiplication on the left cosets of $\mathrm{Gal}(N/k)$ modulo $\mathrm{Gal}(N/E_l)$

for each $l = 1, \dots, s$. The resulting action $\mathrm{Gal}(N/k) \to S_m$ on all these left cosets, which is well-defined up to conjugation by elements of S_m, is called the *Galois representation of* $\prod_{l=1}^{s} E_l/k$ *relative to* N. Equivalently it can be defined as the action of $\mathrm{Gal}(N/k)$ on the set of all k-embeddings $E_l \hookrightarrow N$, $l = 1, \dots, s$.

Conversely, an action $\mu : \mathrm{Gal}(N/k) \to S_m$ determines a k-étale algebra in the following way. For $i = 1, \dots, m$, denote the fixed field in N of the subgroup of $\mathrm{Gal}(N/k)$ consisting of all τ such that $\mu(\tau)(i) = i$ by E_i. The product $\prod_l E_l/k$ for l ranging over a set of representatives of the orbits of the action μ and where each extension E_l/k is regarded modulo k-isomorphism is a k-étale algebra with $\sum_l [E_l : k] = m$.

G-*Galois variant*: if $\prod_{l=1}^{s} E_l/k$ is a *single Galois extension* E/k, the restriction $\mathrm{Gal}(N/k) \to \mathrm{Gal}(E/k)$ is called *the* G-*Galois representation of* E/k (relative to N). Any map $\varphi : \mathrm{Gal}(N/k) \to G$ obtained by composing $\mathrm{Gal}(N/k) \to \mathrm{Gal}(E/k)$ with a monomorphism $\mathrm{Gal}(E/k) \to G$ is called a G-Galois representation of E/k (relative to N). The extension E/k can be recovered from $\varphi : \mathrm{Gal}(N/k) \to G$ by taking the fixed field in N of $\ker(\varphi)$. One obtains the Galois representation $\mathrm{Gal}(N/k) \to S_n$ of E/k (relative to N) from a G-Galois representation $\varphi : \mathrm{Gal}(N/k) \to G$ (relative to N) by composing it with the left-regular representation of the image group $\varphi(\mathrm{Gal}(N/k))$.

2.1.2. *Covers and function field extensions.* Given a regular projective geometrically irreducible k-variety B, a *k-mere cover of B* is a finite and generically unramified morphism $f : X \to B$ defined over k with X a normal and geometrically irreducible variety. Through the function field functor k-mere covers $f : X \to B$ correspond to finite separable field extensions $k(X)/k(B)$ that are regular over k (*i.e.* $k(X) \cap \overline{k} = k$). The Galois group of the Galois closure $\widehat{k(X)}/k(B)$ of $k(X)/k(B)$ is called the *monodromy group* of f and the monodromy group of the k^{sep}-mere cover $f \otimes_k k^{\mathrm{sep}}$ the *geometric monodromy group.* The Galois closure $\widehat{k(X)}/k(B)$ need not be a regular extension of k; it does if and only if the monodromy group and the geometric monodromy group coincide. This happens for example if $\widehat{k(X)} = k(X)$ (*i.e.* if f is Galois), or if f is of degree n and geometric monodromy group S_n. When the Galois closure $\widehat{k(X)}/k(B)$ is regular over k, it corresponds to a Galois k-mere cover $g : Z \to B$ called the Galois closure of f.

The term "mere" used above is meant to distinguish mere covers from G-covers. By k-G-*cover of B of group G*, we mean a Galois cover $f : X \to B$ over k given together with an isomorphism

$G \to \mathrm{Gal}(k(X)/k(B))$. Viewed as a mere cover (*i.e.* without the isomorphism $G \to \mathrm{Gal}(k(X)/k(B))$), $f : X \to B$ is a Galois k-mere cover. G-covers of B of group G over k correspond to regular Galois extensions $k(X)/k(B)$ given with an isomorphism of the Galois group $\mathrm{Gal}(k(X)/k(B))$ with G.

We sometimes abuse terminology and call G-covers (resp. mere covers) *regular Galois covers* (resp. *regular covers*).

By *branch divisor* of a k-cover f (mere or G-), we mean that of the k^{sep}-cover $f \otimes_k k^{\mathrm{sep}}$, *i.e.* the formal sum of all hypersurfaces of B such that the associated discrete valuations are ramified in the extension $k^{\mathrm{sep}}(X)/k^{\mathrm{sep}}(B)$.

2.1.3. *π_1-representations.* Given a reduced positive divisor $D \subset B$, denote the *k-fundamental group* of $B \setminus D$ by $\pi_1(B \setminus D, t)_k$ where $t \in B(\overline{k})\setminus D$ is a base point. Conjoining the two dictionaries covers-function field extensions and field extensions-Galois representations, we obtain the following correspondences.

Mere covers of B of degree n (resp. G-covers of B of group G) with branch divisor contained in D correspond to transitive morphisms $\pi_1(B \setminus D, t)_k \to S_n$ such that the restriction to $\pi_1(B \setminus D, t)_{k^{\mathrm{sep}}}$ is transitive (resp. to epimorphisms $\pi_1(B \setminus D, t)_k \to G$ such that the restriction to $\pi_1(B \setminus D, t)_{k^{\mathrm{sep}}}$ is onto). These morphisms are called *fundamental group representations* (π_1-representations for short) of the corresponding k-covers (mere or G-).

2.1.4. *Specializations.* Each k-rational point $t_0 \in B(k) \setminus D$ provides a section $\mathrm{s}_{t_0} : \mathrm{G}_k \to \pi_1(B \setminus D, t)_k$ to the exact sequence

$$1 \to \pi_1(B \setminus D, t)_{k^{\mathrm{sep}}} \to \pi_1(B \setminus D, t)_k \to \mathrm{G}_k \to 1$$

well-defined up to conjugation by elements in $\pi_1(B \setminus D, t)_{k^{\mathrm{sep}}}$.

If $\phi : \pi_1(B \setminus D, t)_k \to G$ represents a k-G-cover $f : X \to B$, the morphism $\phi \circ \mathsf{s}_{t_0} : \mathrm{G}_k \to G$ is a G-Galois representation. The fixed field in k^{sep} of $\ker(\phi \circ \mathsf{s}_{t_0})$ is the residue field at some/any point above t_0 in the extension $k(X)/k(B)$. We denote it by $k(X)_{t_0}$ and call $k(X)_{t_0}/k$ *the specialization* of the k-G-cover f at t_0.

If $\phi : \pi_1(B \setminus D, t)_k \to S_n$ represents a k-mere cover $f : X \to B$, the morphism $\phi \circ \mathsf{s}_{t_0} : \mathrm{G}_k \to S_n$ is the *specialization representation* of f at t_0. The corresponding k-étale algebra is denoted by $\prod_{l=1}^{s} k(X)_{t_0,l}/k$ and called the *collection of specializations* of f at t_0. Each field $k(X)_{t_0,l}$ is a residue extension at some prime above t_0 in the extension $k(X)/k(B)$ and *vice-versa*; $k(X)_{t_0,l}$ is called *a specialization* of f at t_0. Geometrically the fields $k(X)_{t_0,l}$ correspond to the definition fields of the points in the fiber $f^{-1}(t_0)$ and $\phi\circ \mathsf{s}_{t_0} : \mathrm{G}_k \to S_n$ to the *action* of G_k on these points. The *compositum* in k^{sep} of the Galois closures of all specializations at t_0 is *the* specialization at t_0 of the Galois closure of f.

2.2. **The twisting lemma.** Let k be a field, $f : X \to B$ be a k-mere cover and $\prod_{l=1}^{s} E_l/k$ be a k-étale algebra. The question we address is whether $\prod_{l=1}^{s} E_l/k$ is the collection $\prod_l k(X)_{t_0,l}/k$ of specializations of $f : X \to B$ at some unramified point $t_0 \in B(k)$. Lemma 2.1 gives a sufficient condition for the answer to be affirmative.

2.2.1. *Statement of the twisting lemma.* We assume that $f : X \to B$ is of degree n and geometric monodromy group S_n. Denote the Galois closure of the cover f by $g : Z \to B$, the *compositum* inside k^{sep} of the Galois closures of the extensions E_l/k, $l = 1,\ldots,s$ by N/k. The *twisted cover* $\widetilde{g}^N : \widetilde{Z}^N \to B$ in the statement below is a k-mere cover obtained by twisting the Galois k-mere cover $g : Z \to B$ by the Galois extension N/k. Its precise definition is given in [DG11] and is recalled in §2.2.2; it is in particular a k-model of $g \otimes_k k^{\mathrm{sep}}$.

Twisting lemma 2.1. *Assume $f : X \to B$ is a degree n k-mere cover with geometric monodromy group S_n and $\prod_{l=1}^{s} E_l/k$ is a k-étale algebra with $\sum_{l=1}^{s}[E_l : k] = n$. Then the twisted cover $\widetilde{g}^N : \widetilde{Z}^N \to B$ has the following property. For each unramified point $t_0 \in B(k)$,*

if (i) *there exists a point $x_0 \in \widetilde{Z}^N(k)$ such that $\widetilde{g}^N(x_0) = t_0$,*

then (ii) *$\prod_l E_l/k$ is the collection $\prod_l k(X)_{t_0,l}/k$ of specializations of f at the point t_0.*

For $B = \mathbb{P}^1$, a polynomial form of the statement can be given for which the k-mere cover is replaced by a polynomial $P(T,Y) \in k[T,Y]$ of degree n and with Galois group S_n over $\overline{k}$, as a polynomial in Y. For all but finitely many $t_0 \in k$, implication (i) $\Rightarrow$ (ii) holds with condition (ii) translated as follows:

(ii) *the polynomial $P(t_0, Y)$ factors as a product $\prod_{l=1}^{s} Q_l(Y)$ of polynomials Q_l irreducible in $k[Y]$ and such that E_l/k is generated by one of its roots, $l = 1,\ldots,s$.*

With some adjustments, some converse (ii) $\Rightarrow$ (i) also holds in the twisting lemma 2.1. It is also possible to relax the assumption that the geometric monodromy group of $f : X \to B$ is S_n, at the cost of some technical complications. This is explained in [DL11], together with some specific applications.

2.2.2. *Proof of the twisting lemma.* Let $H = \mathrm{Gal}(N/k)$, $\varphi : \mathrm{G}_k \to H$ be the G-Galois representation of N/k relative to k^{sep} and $\mu : H \to S_n$ be the Galois representation of $\prod_{l=1}^{s} E_l/k$ relative to N. The map $\mu \circ \varphi : \mathrm{G}_k \to S_n$ is then the Galois representation of $\prod_{l=1}^{s} E_l/k$ relative to k^{sep}. Denote the s orbits of $\mu : H \to S_n$, which are the same as the orbits of $\mu \circ \varphi : \mathrm{G}_k \to S_n$, by $\mathcal{O}_1, \ldots, \mathcal{O}_s$; they correspond to the extensions $E_1, \ldots E_s$. Fix one of these orbits, *i.e.* $l \in \{1, \ldots, s\}$, and let $i \in \{1, \ldots, n\}$ be some index such that E_l is the fixed field in k^{sep} of the subgroup of G_k fixing i *via* the action $\mu \circ \varphi$.

As the k-mere cover $f : X \to B$ is of degree n and that the Galois group $\mathrm{Gal}(k^{\mathrm{sep}}(Z)/k^{\mathrm{sep}}(B))$ is assumed to be isomorphic to S_n, the same is true of $\mathrm{Gal}(k(Z)/k(B))$. Therefore $k(Z)$ is a regular extension of k, or, in other words, $g : Z \to B$ is a k-G-cover. Let $\phi : \pi_1(B \setminus D, t)_k \to S_n$ be the corresponding π_1-representation (where D is the branch divisor of f).

With $\mathrm{Per}(S_n)$ the permutation group of S_n, consider the map

$$\widetilde{\phi}^{\mu\varphi} : \pi_1(B \setminus D, t)_k \to \mathrm{Per}(S_n)$$

defined by this formula, where r is the restriction $\pi_1(B \setminus D, t)_k \to \mathrm{G}_k$: for $\theta \in \pi_1(B \setminus D, t)_k$ and $x \in S_n$,

$$\widetilde{\phi}^{\mu\varphi}(\theta)(x) = \phi(\theta)\, x\, (\mu \circ \varphi \circ r)(\theta)^{-1}$$

It is easily checked that $\widetilde{\phi}^{\mu\varphi}$ is a group homomorphism, with the same restriction on $\pi_1(B \setminus D, t)_{k^{\mathrm{sep}}}$ as ϕ (composed with the left-regular representation of S_n). Hence the corresponding action is transitive. Denote the corresponding k-mere cover by $\widetilde{g}^N : \widetilde{Z}^N \to B$ and call it the *twisted cover* of g by the extension N/k; it is a k-model of the k^{sep}-mere cover $g \otimes_k k^{\mathrm{sep}}$. The twisted cover $\widetilde{g}^N : \widetilde{Z}^N \to B$ was defined in [DG11] (and originally in [Dèb99c]) where is also given its main property that we are using below.

Let $t_0 \in B(k) \setminus D$ and assume that condition (i) from lemma 2.1 holds, *i.e.*, there exists $x_0 \in \widetilde{Z}^N(k)$ such that $\widetilde{g}^N(x_0) = t_0$. Then from [DG11, lemma 2.1], there exists $\omega \in S_n$ such that

$$\phi(\mathsf{s}_{t_0}(\tau)) = \omega\, (\mu \circ \varphi)(\tau)\, \omega^{-1} \quad (\tau \in \mathrm{G}_k)$$

where $\mathrm{s}_{t_0} : \mathrm{G}_k \to \pi_1(B \setminus D, t)_k$ is the section associated with t_0 (§2.1.4). It follows that for $j = \omega(i)$, we have, for every $\tau \in \mathrm{G}_k$,

$$\phi(\mathsf{s}_{t_0}(\tau))(j) = \omega\, (\mu \circ \varphi)(\tau)\, (i)$$

and so j is fixed by $\phi(\mathsf{s}_{t_0}(\tau))$ if and only if i is fixed by $(\mu \circ \varphi)(\tau)$. Conclude that the specialization $k(X)_{t_0,j}$ and the field E_l coincide. □

3. Varying the base field

We consider the general problem over various base fields k. We start with the case of PAC fields (§3.1), which after a first result in [Dèb99c], has also been studied in parallel by Bary-Soroker; see [BS10], [BS09, corollary 1.4]. §3.2 is devoted to finite fields for which various forms of the results also exist in the literature. These two cases are presented here as special cases of our unifying approach. §3.3 and §3.4 give newer applications, to the cases k is a complete field and k is a number field.

3.1. **PAC fields.** If k is a PAC field, then condition (i) from lemma 2.1 holds for all t_0 in a Zariski dense subset of $B(k) \setminus D$; consequently so does condition (ii).

Corollary 3.1. *Let k be a PAC field and $f : X \to B$ be a k-mere cover of degree n and geometric monodromy group S_n. If $\prod_{l=1}^{s} E_l/k$ is a k-étale algebra with $\sum_{l=1}^{s}[E_l : k] = n$, then for all t_0 in a Zariski dense subset of $B(k) \setminus D$, the collection $\prod_l k(X)_{t_0,l}/k$ of specializations of f at t_0 is $\prod_l E_l/k$.*

A similar result is [BS10, theorem 2.4]. As a special case we obtain this statement, which is also [BS09, corollary 1.4]: if $P(T,Y) \in k[T,Y]$ is a polynomial of degree n and Galois group S_n over $\overline{k}$, as a polynomial in Y and E/k is a degree n separable extension, then there exist infinitely many $t_0 \in k$ such that $P(t_0,Y)$ is irreducible in $k[Y]$ and has a root in $\overline{k}$ that generates E/k.

3.2. **Finite fields.** Assume $k = \mathbb{F}_q$ is the finite field of order q and as above consider the case of covers of $\mathbb{P}^1$ (for simplicity). From the Lang-Weil estimates for the number of rational points on a curve over $\mathbb{F}_q$, condition (i) from lemma 2.1 holds for at least one unramified $t_0 \in k$ if $q + 1 - 2\widetilde{\mathrm{g}}\sqrt{q} > \widetilde{r}n!$ where $\widetilde{\mathrm{g}}$ is the genus of the covering space $\widetilde{Z}^N$ of the mere cover $\widetilde{g}^N$ from lemma 2.1 and $\widetilde{r}$ the branch point number of $\widetilde{g}^N$. But $\widetilde{g}^N \otimes_k k^{\mathrm{sep}} \simeq g \otimes_k k^{\mathrm{sep}}$ (where $g : Z \to \mathbb{P}^1$ is as before the Galois closure of $f : X \to \mathbb{P}^1$). Consequently $\widetilde{r}$ is merely the branch point number of f and $\widetilde{\mathrm{g}}$ the genus of $g : Z \to \mathbb{P}^1$. Using the Riemann-Hurwitz formula, it is readily checked that $q \geq 4r^2(n!)^2$ suffices to guarantee the preceding inequality. We obtain the following.

Corollary 3.2. *Let $f : X \to \mathbb{P}^1$ be a $\mathbb{F}_q$-mere cover of degree n, with r branch points and with geometric monodromy group S_n. Assume that $q \geq 4r^2(n!)^2$. Then for every positive integers $d_1, \ldots, d_s$ (possibly* *repeated) such that $\sum_{l=1}^{s} d_l = n$, there exists at least one $t_0 \in \mathbb{F}_q$ such that $\prod_{l=1}^{s} \mathbb{F}_{q^{d_l}}/\mathbb{F}_q$ is the collection of specializations of f at t_0.*

One can even evaluate the number of $t_0 \in \mathbb{F}_q$ for which the conclusion holds: for example for $s = 1$ and $d_1 = n$, it is of the form $q/n + O(\sqrt{q})$. See [DL11] for details on this extra conclusion (which uses the converse (ii) ⇒ (i) in the twisting lemma alluded to in §2.2.1).

3.3. **Complete valued fields.**

Assume k is the quotient field of some complete discrete valuation ring A. Denote the valuation ideal by $\mathfrak{p}$, the residue field by κ, assumed to be perfect, and its characteristic by $p \geq 0$. A k-étale algebra $\prod_{l=1}^{s} E_l/k$ is said to be *unramified* if each field extension E_l/k is unramified.

Let B be a smooth projective and geometrically irreducible k-variety given with an integral smooth projective model $\mathcal{B}$ over A. Let $f : X \to B$ be a degree n k-mere cover with branch divisor D. Denote the Zariski closure of D in $\mathcal{B}$ by $\mathcal{D}$, the normalization of $\mathcal{B}$ in $k(X)$ by $\mathcal{F} : \mathcal{X} \to \mathcal{B}$ and its special fiber by $\mathcal{F}_0 : \mathcal{X}_0 \to \mathcal{B}_0$.

The constant $c(f, \mathcal{B})$ in the statement below only depends on f and $\mathcal{B}$. It is the constant $c(g, \mathcal{B})$ from [DG11] for $g : Z \to B$ the Galois closure of $f : X \to B$. For $B = \mathbb{P}^1$, it can be taken to be $c(f, \mathcal{B}) = 4r^2(n!)^2$ where r is the branch point number of f. See [DG11, §2.5] for a more general description.

Corollary 3.3. *Let k, $\mathcal{B}$ and $f : X \to B$ be as above and $\prod_{l=1}^{s} E_l/k$ be an unramified k-étale algebra with $\sum_{l=1}^{s}[E_l : k] = n$. Assume that the geometric monodromy group of $f : X \to B$ is S_n and that these two further conditions hold:*

(good-red) *$p = 0$ or $p > n$, $\mathcal{D}$ is smooth, $\mathcal{D} \cup \mathcal{B}_0$ is regular with normal crossings over A, and there is no vertical ramification at $\mathfrak{p}$ in the Galois closure $g : Z \to B$*[2]*.*

(κ-big-enough) *κ is a PAC field or is a finite field of order $q \geq c(f, \mathcal{B})$.*

Then there exist points $t_0 \in B(k) \setminus D$ such that $\prod_{l=1}^{s} E_l/k$ is the collection of specializations of f at t_0. More precisely, the set of such points t_0 contains the preimage via the map $\mathcal{B}(A) \to \mathcal{B}_0(\kappa)$ of a non-empty subset $F \subset \mathcal{B}_0(\kappa) \setminus \mathcal{D}_0$.

[2] see [DG11] for a precise definition of non-vertical ramification. This condition can in fact be removed here if $n \geq 3$: according to a lemma of Beckmann [Bec91], no vertical ramification may then occur (under the other assumptions $p > n$ and $\mathcal{D}$ étale) as the geometric monodromy group S_n is of trivial center.

Proof. Let $\widetilde{g}^N : \widetilde{Z}^N \to B$ be the k-mere cover from lemma 2.1, obtained by twisting the Galois closure $g : Z \to B$ of $f : X \to B$ by the *compositum* N/k of the Galois closures of $E_1/k, \ldots, E_s/k$. From lemma 2.1, it suffices to show that $\widetilde{Z}^N$ has k-rational points. This (and the more precise conclusion of corollary 3.3) is explained in proposition 2.2 and lemma 2.4 from [DG11] which we summarize below.

Denote by $\mathcal{G} : \mathcal{Z} \to \mathcal{B}$ the normalization of $\mathcal{B}$ in $k(Z)$. Assumption (good-red) holds for $\mathcal{G}$ as it holds for $\mathcal{F}$ (f and g have the same branch divisor) and the Galois extension N/k is unramified (*compositum* of unramified extensions). These two conditions guarantee that the morphism $\widetilde{\mathcal{G}}^N : \widetilde{\mathcal{Z}}^N \to \mathcal{B}$ obtained by normalizing $\mathcal{B}$ in $k(\widetilde{Z}^N)$ has good reduction (including no vertical ramification at $\mathfrak{p}$) [DG11, proposition 2.2]. Assumption (κ-big-enough) shows next that κ-rational points exist on the special fiber $\widetilde{\mathcal{Z}}^N_0$; if κ is finite, this follows from the Lang-Weil estimates [DG11, lemma 2.4]. Hensel's lemma is finally used to lift these κ-rational points to k-points on $\widetilde{Z}^N$. □

3.4. **Local-global results.** Finding rational points on varieties over a global field k is harder than it is over local fields. Nevertheless results from §3.3 can be used to obtain local-global statements. We explain below how to globalize local information coming from corollary 3.3.

Let k be the quotient field of some Dedekind domain R and S be a finite set of places of k corresponding to some prime ideals in R. For every place v, the completion of k is denoted by k_v, the valuation ring by R_v, the valuation ideal by $\mathfrak{p}_v$, the residue field by κ_v which we assume to be perfect, the order (possibly infinite) of κ_v by q_v and its characteristic by p_v.

Let B be a smooth projective and geometrically integral k-variety, given with an integral model $\mathcal{B}$ over R such that $\mathcal{B}_v = \mathcal{B} \otimes_R R_v$ is smooth for each $v \in S$. The *weak approximation property* below guarantees that k_v-rational points on B ($v \in S$) that may be provided by corollary 3.3 can be approximated by some k-rational point on B.

(weak-approx $/S$) *$B(k)$ is dense in $\prod_{v\in S} B(k_v)$.*

The next statement then readily follows from corollary 3.3.

Corollary 3.4. *Let k, S, $\mathcal{B}$ be as above, $f : X \to B$ be a degree n k-mere cover with branch divisor D, and, for each $v \in S$, let $\prod_{l=1}^{s_v} E_{v,l}/k_v$ be an unramified k_v-étale algebra with $\sum_{l=1}^{s_v}[E_{v,l} : k_v] = n$.*

Assume that

- the geometric monodromy group of $f : X \to B$ is S_n,

- the weak approximation condition (weak-approx $/S$) *holds, and*

- *for each $v \in S$, assumptions* (good-red) *and* (κ-big-enough) *of corollary 3.3 hold for the k_v-mere cover $f \otimes_k k_v$ and the residue field κ_v.*

Then there exist v-adic open subsets $U_v \subset B(k_v) \setminus D$ ($v \in S$) such that $B(k) \cap \prod_{v\in S} U_v \neq \emptyset$ and the following holds: for each $t_0 \in B(k) \cap \prod_{v\in S} U_v$ and each $v \in S$, the étale algebra $\prod_{l=1}^{s_v} E_{v,l}/k_v$ is the collection of specializations of $f \otimes_k k_v$ at t_0.

Addendum 3.4. Each condition $q_v \geq c(f \otimes_k k_v, \mathcal{B} \otimes_k k_v)$ from assumption (κ_v-big-enough) can be guaranteed by some condition $q_v \geq C(f, \mathcal{B})$ where $C(f, \mathcal{B})$ only depends on f and $\mathcal{B}$ (and not on v). This constant is the constant $C(g, \mathcal{B})$ from [DG11] with g the Galois closure of f. For $B = \mathbb{P}^1$, it can be taken to be $C(f, \mathcal{B}) = 4r^2(n!)^2$ where r is the branch point number of f. See [DG11, §3.1] for a more general description.

4. Applications

The three subsections of this section correspond to the three main applications presented in the introduction.

4.1. **Hilbert's irreducibility theorem.**

We elaborate on the local-global results from §3.4 when $B = \mathbb{P}^1$. In this situation, assumption (weak-approx $/S$) holds for every S and the good reduction assumption (good-red) requires that each place $v \in S$ be *good*, by which we mean that $p_v = 0$ or $p_v > n$, *the branch point set* $\mathbf{t} = \{t_1, \ldots, t_r\}$ *of f is étale* (*i.e.*, no two distinct branch points *coalesce* modulo the valuation ideal of v) and there is no vertical ramification in the Galois closure of f [3].

4.1.1. *A standard trick.* Over certain fields (*e.g.* number fields), there is a trick that makes it possible, at the cost of throwing in more places in S, to further guarantee in corollary 3.4 that Hilbert's irreducibility conclusion holds, *i.e.* that the collection of specializations of f at t_0 consists of a single field extension $k(X)_{t_0}/k$ of degree n.

Namely the idea is to construct a finite set S_0 of finite places of k, disjoint from S, and to attach to each $v \in S_0$ a k_v-étale algebra $\prod_l E_{v,l}/k_v$ with all $E_{v,l}/k_v$ trivial but one consisting of an unramified Galois extension E_v/k_v of group H_v of order $\leq n$. If the assumptions of corollary 3.4 still hold for the set $T = S \cup S_0$, then it follows from its conclusion that $\mathrm{Gal}(k(Z)_{t_0}/k)$ contains some conjugate subgroup $H_v^{g_v}$ of H_v for some $g_v \in S_n$ ($v \in S_0$). In some situations, this last condition implies that $\mathrm{Gal}(k(Z)_{t_0}/k)$ is all of S_n. This is the case for example if S_0 contains 3 places with corresponding H_v cyclic subgroups respectively

[3] This last condition is automatic if the geometric monodromy group is S_n with $n = \deg(f) \geq 3$.

generated by a n-cycle, a $n-1$-cycle and a 2-cycle. Of course, for this idea to work, Galois extensions E_v/k_v with groups H_v should exist, for places v satisfying the assumptions of corollary 3.4.

4.1.2. *The number field case.* We develop the number field case for which this trick can be used. Another example would be to work over $k = \kappa(x)$ with κ a PAC field with enough cyclic extensions. We will also use the explicit aspect of [DG11] that makes it possible to be more precise on the constants. For simplicity take $k = \mathbb{Q}$. The next statement is the outcome of the above considerations, together with corollary 3.4 (a detailed proof is easily obtained by adjusting the proof of [DG11, corollary 4.1]).

Corollary 4.1. *Let $f : X \to \mathbb{P}^1$ be a degree n $\mathbb{Q}$-mere cover with geometric monodromy group S_n. There exist integers $m_0, \beta > 0$ depending on f with the following property. Let $\mathcal{S}$ be a finite set of good primes $p > m_0$, each given with positive integers $d_{p,1} \ldots, d_{p,s_p}$ (possibly repeated) with $\sum_{l=1}^{s_p} d_{p,l} = n$. Then there exists $b \in \mathbb{Z}$ such that*

(i) $0 \leq b \leq \beta \prod_{p\in\mathcal{S}} p$,

(ii) *for each integer $t_0 \equiv b \bmod (\beta \prod_{p\in\mathcal{S}} p)$, t_0 is not a branch point of f and the collection of specializations of f at t_0 consists of a single field extension $\mathbb{Q}(X)_{t_0}/\mathbb{Q}$ of degree n which has residue degrees $d_{p,1} \ldots, d_{p,s_p}$ at p for each $p \in \mathcal{S}$, and S_n as Galois group of its Galois closure.*

Addendum 4.1 (on the constants) Denote the number of branch points of f by r and the number of bad primes by $\mathrm{br}(\mathbf{t})$. One can take m_0 such that the interval $[4r^2(n!)^2, m_0]$ contains at least $\mathrm{br}(\mathbf{t}) + 3$ distinct primes, and β to be the product of 3 good primes in $[4r^2(n!)^2, m_0]$.

If the cover $f : X \to \mathbb{P}^1$ is given by a polynomial $P(T, Y) \in \mathbb{Q}[T, Y]$, addendum 4.1 provides a bound for the least specialization $t \geq 0$ making $P(t, Y)$ irreducible in $\mathbb{Q}[Y]$ that depends only on $\deg_Y(P)$, r and $\mathrm{br}(\mathbf{t})$. It is conjectured that a bound depending only on $\deg(P)$ exists in general for Hilbert's irreducibility theorem (see [DW08]).

4.2. **Trinomial realizations and variants.** Bary-Soroker's motivation in [BS09] was to obtain analogs of Dirichlet's theorem for polynomial rings. He proved that if k is a PAC field, then given $a(Y), b(Y) \in k[Y]$ relatively prime, for every integer n, suitably large (depending on $a(Y), b(Y)$) and for which k has at least one degree n separable extension, there are infinitely many $c(Y) \in k[Y]$ such that $a(Y)+b(Y)c(Y) \in k[Y]$ is irreducible and of degree n. The strategy is to construct $c_0(Y) \in k[Y]$ such that $a(Y) + b(Y)c_0(Y)T \in k[T, Y]$ is absolutely irreducible, of degree n and Galois group S_n over $\overline{k}(T)$, and then to specialize t properly (as in §3.1). We develop below other applications.

4.2.1. *Classical regular realizations of* S_n. An hypothesis in our results from §3 is that the k-mere cover $f : X \to B$ is of degree n and of geometric monodromy group S_n. We recall below some classical covers $f : X \to \mathbb{P}^1$ with these properties. The cover f is given by a polynomial $P(T,Y) \in k[T,Y]$, the map f corresponding to the T-projection $(t,y) \to t$ from the curve $P(t,y) = 0$ to the line. Fix the integer $n \geq 2$.

(a) (*Trinomials*): k is a field and $P(T,Y) = Y^n - T^r Y^m + T^s \in k[T,Y]$ where n, m, r, s are positive integers such that $1 \leq m < n$, $(m,n) = 1$, the characteristic $p \geq 0$ of k does not divide $mn(m-n)$ and $s(n-m) - rn = 1$. The branch points of the associated cover $f : X \to \mathbb{P}^1$ are 0, ∞ and $t_0 = m^m n^{-n}(n-m)^{n-m}$ with corresponding ramification indices $m(n-m)$ at 0, n at ∞ and 2 at t_0. See [Sch00, §2.4].

There are other classical trinomials realizing S_n; see [Ser92, §4.4]:
- $P(T,Y) = Y^n - Y^{n-1} - T$ for p not dividing $n(n-1)$, which has branch points $0, \infty, Q(1-(1/n))$ with $Q(Y) = Y^n - Y^{n-1}$, and ramification indices n at ∞, $n-1$ at 0 and 2 at $Q(1-(1/n))$,
- $P(T,Y) = Y^n - Y - T$ for p not dividing $n(n-1)$; this last example is a special case of (b) below.

(b) (*Morse polynomials*): k is of characteristic $p \geq 0$ not dividing n and $P(T,Y) = M(Y) - T$ where $M(Y) \in k[Y]$ is a degree n *Morse polynomial*, that is: the zeroes $\beta_1, \ldots, \beta_{n-1}$ of the derivative M' are simple and $M(\beta_i) \neq M(\beta_j)$ for $i \neq j$. The branch points of the cover $f : X \to \mathbb{P}^1$ are ∞ and $M(\beta_1), \ldots, M(\beta_{n-1})$, with ramification indices n at ∞ and 2 at $M(\beta_1), \ldots, M(\beta_{n-1})$. See [Ser92, §4.4].

(c) (*An example of Uchida*): Let k be any field and $U_0, \ldots, U_3$ be 4 algebraically independent indeterminates. It is proved in [Uch70, corollary 2] that for every $n \geq 4$, the polynomial $F(Y) = Y^n + U_3Y^3 + U_2Y^2 + U_1Y + U_0$ has Galois group S_n over the field $k(U_0, \ldots, U_3)$. The following lemma makes it possible to derive a polynomial

$$P(T,Y) = Y^n + u_3(T)Y^3 + u_2(T)Y^2 + u_1(T)Y + u_0(T) \in k[T,Y]$$

of Galois group S_n over $\overline{k}(T)$.

Lemma 4.2. *Let* $\underline{U} = (U_1, \ldots, U_\ell)$ *be a set of algebraically independent indeterminates and* $F(\underline{U}, Y) \in k(\underline{U})[Y]$ *be a degree* n *polynomial with Galois group* S_n *over* $\overline{k}(\underline{U})$. *Then there exist infinitely many* ℓ*-tuples* $\underline{u}_T = (u_1(T), \ldots, u_\ell(T)) \in k[T]^\ell$ *such that the polynomial* $F(\underline{u}_T, Y)$ *has Galois group* S_n *over* $\overline{k}(T)$.

Proof. The polynomial $F(\underline{U}, Y)$ has Galois group S_n over the field $\overline{k}(T)(\underline{U})$. The desired conclusion follows from the Hilbert specialization property of the hilbertian field $\overline{k}(T)$ but one needs a version that provides good specialisations in $k(T)$ (and not just in $\overline{k}(T)$). This is classical if k is infinite (*e.g.* [FJ04, §13.2]). For the general case, we resort to theorem 3.3 from [Dèb99b] which shows that given a Hilbert subset $\mathcal{H} \subset \overline{k}(T)$, for all but finitely many $t_0 \in \overline{k}(T)$, there exists $a \in \overline{k}(T)$ such that if $b \in k[T]$ is any non-constant polynomial, then $\mathcal{H}$ contains infinitely many elements of the form $t_0 + ab^m$ $(m \geq 0)$. This gives what we want if a can be chosen in $k(T)$. Although this is not stated, the proof shows that such a choice is possible; the main point is to adjust [Dèb99b, lemma 3.2] to show that there are infinitely many cosets of $k(T)$ modulo $\overline{k}(T)^p$, where p is the characteristic of k. □

4.2.2. *Special realizations of extensions of PAC fields.* We say a field extension E/k can be *realized by a polynomial* $Q(Y) \in k[Y]$ if $Q(Y)$ is the irreducible polynomial over k of some primitive element of E/k.

Corollary 4.3. *Let k be a PAC field of characteristic $p \geq 0$. If $n \geq 2$ and p does not divide $n(n-1)$, every degree n extension E/k can be realized by a trinomial $Y^n - Y + b$ for some $b \in k$. Furthermore, if $p \neq 2$, the separable closure k^{sep} is generated over k by all elements $y \in k^{\mathrm{sep}}$ such that $y^n - y \in k$ for some integer $n \geq 2$.*

Proof of corollary 4.3. The first part follows from corollary 3.1 applied with $f : X \to \mathbb{P}^1$ given by the trinomial $P(T, Y) = Y^n - Y - T$ from §4.2.1 (a) and the étale algebra $\prod_{l=1}^{s} E_l/k$ taken to be the field extension E/k. To prove the second part, consider a separable extension E/k of degree $m \geq 2$. Pick an integer $n \geq m$ such that p does not divide $n(n-1)$ (this is possible as $p \neq 2$) and do as above but with the étale algebra $\prod_{l=1}^{s} E_l/k$ taken to be the product of the field extension E/k with $n-m$ copies of the trivial extension k/k. Conclude that E/k has a primitive element whose irreducible polynomial divides $Y^n - Y + b$ for some $b \in k$. As E/k is an arbitrary finite extension, this provides the announced description of k^{sep}. □

Proceeding as above but using the Morse polynomial realization (b) from §4.2.1 (instead of trinomial realizations), we obtain this statement.

Corollary 4.4. *Let $n \geq 2$ be an integer, k be a PAC field of characteristic $p \geq 0$ not dividing n and $M(Y) \in k[Y]$ be a degree n Morse polynomial. Then every degree n extension E/k can be realized by a polynomial $M(Y) + b$ for some $b \in k$.*

Finally Uchida's example and lemma 4.2 from §4.2.1 (c) yield this.

Corollary 4.5. *Let $n \geq 4$ be an integer and k be a PAC field of any characteristic. Then every separable degree n extension E/k can be realized by a polynomial $Y^n + aY^3 + bY^2 + cY + d$ for some $a, b, c, d \in k$.*

4.2.3. *Variants.*

(a) *Finite fields.* Proceeding as above but using corollary 3.2 instead of corollary 3.1 leads to the following conclusions for finite fields:

- *if $n \geq 2$ and $q \geq (2nn!)^2$ is a prime power with $(q, n(n-1)) = 1$, the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ can be realized by a trinomial $Y^n - Y + b \in \mathbb{F}_q[Y]$,*
- *if $M(Y) \in \mathbb{F}_q[Y]$ is a degree n Morse polynomial such that $(n, q) = 1$ and $q \geq (2nn!)^2$, the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ can be realized by the polynomial $M(Y) + b$ for some $b \in \mathbb{F}_q$.*

(b) *p-adic fields.* It follows from (a) that

- *if $p \geq (2nn!)^2$ is a prime, the degree n unramified extension of $\mathbb{Q}_p$ can be realized by a trinomial $Y^n - Y + b$ for some $b \in \mathbb{Z}_p$, or by a polynomial $M(Y) + b$ with $b \in \mathbb{Z}_p$ and $M(Y) \in \mathbb{Z}_p[Y]$ a degree n monic polynomial with reduction modulo p a Morse polynomial in $\mathbb{F}_p[Y]$.*

This can also be proved by using §3.3 instead of §3.2 (with possibly another bound on p).

(c) *Other trinomials.* The trinomials $Y^n - Y^{n-1} - T$ and $Y^n - T^rY^m + T^s$ from §4.2.1 can be used instead of $Y^n - Y - T$ to provide similar conclusions. The assumption on p remains that $p \not| n(n-1)$ for the former, and for the latter, it is that $p \not| mn(n-m)$ (with the other conditions on n and m from §4.2.1); and the bound on q can be replaced by the better one $q = p^f \geq (6n!)^2$.

(d) *Missing characteristics.* Given an integer $n \geq 2$ and a prime p, corollary 3.1, combined with lemma 4.2, shows in fact that

(*) *every degree n separable extension E/k of a PAC field k of characteristic p can be realized by some trinomial $Y^n + aY^m + b$ for some integer $1 \leq m < n$ and some $a, b \in k$,*

provided that the following holds:

(**) *there exists $1 \leq m < n$ such that the trinomial $Y^n + UY^m + V$ has Galois group S_n over $\overline{\mathbb{F}}_p(U, V)$ (where U, V are two indeterminates).*

There are many results about condition (**) in the literature, notably in the papers [Uch70], [Coh80] and [Coh81]. Here are conclusions that can be derived about the cases not covered by corollary 4.3:

- if $p \neq 2$, ($p|n$ or $p|n-1$) and n is odd, (**) holds with $Y^n + UY^2 + V$ or with $Y^n - UY + V$ ([Coh81, corollary 3] and [Uch70, theorem2]),

- if $p = 2$ and n is odd, (**) holds with $Y^n + UY^2 + V$ if $n \geq 5$ [Coh81, corollary 3] and with $Y^n - UY + V$ if $n = 3$ [Uch70, theorem2],
- if $p = 3$ and $n = 4$, (**) holds with $Y^n - UY + V$ [Uch70, theorem2],
- if ($p = 5$ and $n = 6$) or ($p = 2$ and $n = 6$), (**) does not hold: $Y^6 - UY + V$ has Galois group $\mathrm{PGL}_2(\mathbb{F}_5)$ over $\mathbb{F}_5(U, V)$ and $Y^6 - UY + V$ has Galois group A_5 over $\mathbb{F}_4(U, V)$ [Uch70].

Note that conjoining these results with corollary 4.3, we obtain that (**) and (*) always hold if n is odd.

(e) *Number fields.* Over a number field k, extensions with trinomial realizations are more sparse. For example, Angeli proved that, for every $n \geq 3$, there are (up to some standard equivalence for trinomials) only finitely many degree n trinomials with coefficients in k, irreducible and with Galois group a primitive subgroup $G \subset S_n$ distinct from S_n and A_n [Ang09]. See also [Ang07] where the same is proved with "$G \subset S_n$ primitive" replaced by "G solvable" in the case n is a prime.

4.3. **Hurwitz spaces.** Given an integer $r \geq 3$ and a finite group G (resp. a subgroup $G \subset S_n$), there is a coarse moduli space called *Hurwitz space* for G-covers of $\mathbb{P}^1$ of group G (resp. for mere covers of $\mathbb{P}^1$ of degree n and geometric monodromy group $G \subset S_n$) with r branch points. We view it here as a (reducible) variety defined over $\mathbb{Q}$; it can be more generally defined as a scheme over some extension ring of $\mathbb{Z}[1/|G|]$. We do not distinguish between the G-cover and mere cover situations and use the same notation $\mathsf{H}_r(G)$ for the Hurwitz space.

A central moduli property is that for any field k of characteristic 0, there is a one-one correspondence between the set of $\overline{k}$-rational points on $\mathsf{H}_r(G)$ and the set of isomorphisms classes of (G- or mere) covers defined over $\overline{k}$ with the given invariants. Furthermore for every closed point $[f] \in \mathsf{H}_r(G)$, the field $k([f])$ is the field of moduli of the corresponding (G- or mere) cover f. We refer to [DD97] for more on fields of moduli; in standard situations (*e.g.* $Z(G) = \{1\}$ for G-covers, $\mathrm{Cen}_{S_n}(G) = \{1\}$ for mere covers) and in most situations below, the field of moduli is a field of definition of f and is the smallest one.

Denote by U_r the configuration space for finite subsets of $\mathbb{P}^1$ of cardinality r. The map $\Psi_r : \mathsf{H}_r(G) \to \mathsf{U}_r$ that sends each isomorphism class of cover $[f]$ in $\mathsf{H}_r(G)$ to its branch point set $\mathbf{t} \in \mathsf{U}_r$ is an étale cover defined over $\mathbb{Q}$. The geometrically irreducible components of $\mathsf{H}_r(G)$ correspond to the connected components of $\mathsf{H}_r(G) \otimes_{\mathbb{Q}} \mathbb{C}$, which in turn correspond to the orbits of the so-called *Hurwitz monodromy action*, of the fundamental group of U_r (the *Hurwitz group* $\mathcal{H}_r$) on a fiber $\Psi_r^{-1}(\mathbf{t})$ ($\mathbf{t} \in \mathsf{U}_r(\overline{k})$). For more on Hurwitz spaces, see [Völ96] or [Dèb99a].

In this situation we have this result. In (b) (ii) where k is a number field and v is a place of k, we use the notation $k_v^{\mathrm{ur},f}$ ($f \in \mathbb{N}, f > 0$) for the unramified extension of k_v of degree f.

Corollary 4.6. *Let H be a component of $\mathsf{H}_r(G)$ defined over a field k and such that the restriction $(\Psi_r)_{\mathsf{H}} : \mathsf{H} \to \mathsf{U}_r$ induces a k-mere cover of geometric monodromy group S_N with $N = \deg((\Psi_r)_{\mathsf{H}})$.*

(a) *If k is PAC of characteristic 0 and $\prod_{l=1}^s E_l/k$ a k-étale algebra with $\sum_{l=1}^s [E_l : k] = N$, there exists a Zariski-dense subset $\mathcal{U} \subset \mathsf{U}_r(k)$ such that for each $\mathbf{t}_0 \in \mathcal{U}$, the k-étale algebra $\prod_{l=1}^s E_l/k$ is the collection of the smallest fields of definition of the $\overline{k}$-covers $[f : X \to \mathbb{P}^1]$ in H (mere or G-) with branch divisor $\mathbf{t}_0$.*

(b) *If k is a number field, there exist two constants $p(r, G)$ and $q(r, G)$ depending only on r and G with the following property. Let S be a finite subset of finite places of k with residue field of order $\geq q(r, G)$ and residue characteristic $\geq p(r, G)$, and for each $v \in S$, let $d_{v,1} \ldots, d_{v,s_v}$ be positive integers with $\sum_{l=1}^{s_v} d_{v,l} = N$. There exists a Zariski-dense subset $\mathcal{U} \subset \mathsf{U}_r(k)$, of the form $\mathcal{U} = \mathsf{U}_r(k) \cap \prod_{v\in S} U_v$ for some v-adic open subsets $U_v \subset \mathsf{U}_r(k_v)$, such that for each $\mathbf{t}_0 \in \mathcal{U}$, the $\overline{k}$-covers $f : X \to \mathbb{P}^1$ in H with branch divisor $\mathbf{t}_0$ satisfy the following:*

(i) *their field of moduli $k([f])$ is a degree N extension of k, and*

(ii) *for each $v \in S$, the k_v-étale algebra $\prod_{l=1}^{s_v} k_v^{\mathrm{ur},d_{v,l}}/k_v$ is the collection of the smallest fields of definition of the $\overline{k_v}$-covers $f \otimes_{\overline{k}} \overline{k_v}$ (for any given embedding $\overline{k} \hookrightarrow \overline{k_v}$).*

Proof. (a) and (b) respectively follow from the twisting lemma 2.1, applied to the k-mere cover $(\Psi_r)_{\mathsf{H}} : \mathsf{H} \to \mathsf{U}_r$, and from the interpretation recalled above of the specializations of this cover at some point $\mathbf{t}_0 \in \mathsf{U}_r$ as the fields of moduli of the points $[f] \in \mathsf{H}$ above $\mathbf{t}_0$. Over a PAC field, the field of moduli is always a field of definition (and is the smallest one) [DD97]. The PAC situation in (a) offers no further difficulty.

Statement (b) is a local-global statement as in §3.4. Conditions $p_v \geq p(r, G)$ and $q_v \geq q(r, G)$ ($v \in S$) are here to guarantee assumptions (good-red) and (κ-big-enough) of corollary 3.4. Condition (good-red) also implies that the field of moduli of each local cover $f \otimes_{\overline{k}} \overline{k_v}$ is a field of definition [DH98]. The variety U_r being birational to $\mathbb{P}^r$ has the weak approximation property (weak-approx $/S$) for any set S, so sets of the form $\mathcal{U} = \mathsf{U}_r(k) \cap \prod_{v\in S} U_v$ with $U_v \subset \mathsf{U}_r(k_v)$ non-empty v-adic open subsets, are non-empty, and even Zariski-dense in $\mathsf{U}_r(k)$. The standard trick recalled in §4.1.1 should be used to obtain condition (ii) that the extension $k([f])/k$ be exactly of degree N. □

There is in corollary 4.6 the assumption that $(\Psi_r)_{\mathsf{H}} : \mathsf{H} \to \mathsf{U}_r$ be a k-mere cover of geometric monodromy group S_N. This assumption can be checked in practical situations. Indeed the geometric monodromy group is the image group of the Hurwitz monodromy action (restricted to the component H), which can be made totally explicit.

References

[Ang07] Julien Angeli. Trinômes irréductibles résolubles sur un corps de nombres. *Acta Arith.*, 127(2):169–178, 2007.

[Ang09] Julien Angeli. *Trinômes à petits groupes de Galois.* Thèse de doctorat, Université de Limoges, 2009.

[Bec91] Sybilla Beckmann. On extensions of number fields obtained by specializing branched coverings. *J. Reine Angew. Math.*, 419:27–53, 1991.

[BS09] Lior Bary-Soroker. Dirichlet's theorem for polynomial rings. *Proc. Amer. Math. Soc.*, 137:73–83, 2009.

[BS10] Lior Bary-Soroker. Irreducible values of polynomials. *manuscript*, 2010.

[Coh80] Stephan D. Cohen. The Galois group of a polynomial with two indeterminate coefficients. *Pacific J. Math.*, 90(1):63–76, 1980.

[Coh81] Stephan D. Cohen. Corrections to [Coh80]. *Pacific J. Math.*, 97(2):483–486, 1981.

[DD97] Pierre Dèbes and Jean-Claude Douai. Algebraic covers: field of moduli versus field of definition. *Annales Sci. E.N.S.*, 30:303–338, 1997.

[Dèb99a] Pierre Dèbes. Arithmétique et espaces de modules de revêtements. In *Number Theory in Progress, (K. Gyory, H. Iwaniec and J. Urbanowicz ed.)*, pages 75–102. Walter de Gruyter, 1999.

[Dèb99b] Pierre Dèbes. Density results for Hilbert subsets. *Indian J. Pure and Applied Math.*, 30(1):109–127, 1999.

[Dèb99c] Pierre Dèbes. Galois covers with prescribed fibers: the Beckmann-Black problem. *Ann. Scuola Norm. Sup. Pisa,* Cl. Sci. (4), 28:273–286, 1999.

[Dèb09] Pierre Dèbes. Arithmétique des revêtements de la droite. 2009. at http://math.univ-lille1.fr/˜pde/ens.html.

[DG11] Pierre Dèbes and Nour Ghazi. Galois covers and the Hilbert-Grunwald property. *Ann. Inst. Fourier*, 61, 2011.

[DH98] Pierre Dèbes and David Harbater. Fields of definition of p-adic covers. *J. Reine Angew. Math.*, 498:223–236, 1998.

[DL11] Pierre Dèbes and François Legrand. Twisted covers and specializations. *preprint*, 2011.

[DW08] Pierre Dèbes and Yann Walkowiak. Bounds for Hilbert's irreducibility theorem. *Pure & Applied Math. Quarterly*, 4/4:1059–1083, 2008.

[FJ04] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete.* Springer-Verlag, Berlin, 2004. (first edition 1986).

[Sch00] Andrzej Schinzel. *Polynomials with special regard to reducibility*, volume 77 of *Encyclopedia of Mathematics and its Applications.* Cambridge University, 2000.

[Ser92] Jean-Pierre Serre. *Topics in Galois Theory.* Research Notes in Mathematics. Jones and Bartlett Publishers, 1992.

[Uch70] Koji Uchida. Galois group of an equation $x^n - ax + b = 0$. *Tohoku Math. Journ.*, 22:670–678, 1970.

[Völ96] Helmut Völklein. *Groups as Galois Groups*, volume 53 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 1996.

E-mail address: Pierre.Debes@math.univ-lille1.fr
E-mail address: Francois.Legrand@math.univ-lille1.fr

Laboratoire Paul Painlevé, Mathématiques, Université Lille 1, 59655 Villeneuve d'Ascq Cedex, France